IA OPSEC Vulnerabilities Can Aid Enemy

September 2005

The bottom line is Operational Security (OPSEC) via Information Assurance (IA) saves soldiers' lives, perhaps even your own. This month's "On Cyber Patrol" brings this point home with the clear message that unsecured transmissions are continuously monitored by opposing forces.

Some might think that the soldier in the cartoon was demonstrating initiative and resourcefulness by overcoming the fact that the secure communications system was down. In fact, he put lives at risk and helped someone win "insurgent of the month." IMs and e-mails home with descriptions of deployment and operations, especially photographs and video, create vulnerabilities. Photos from US troops showing damage to vehicles have turned up in enemy training materials highlighting what they consider might be weaknesses in our defensive systems.

As defined in AR 25-2, "OPSEC is a process of identifying critical information and subsequently analyzing friendly actions attendant to defense acquisition, defense activities, military operations, and other activities to: (a) Identify those actions that may be observed by adversary intelligence systems; (b) Determine what indicators hostile intelligence systems may obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and (c) Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation."

Transmitting any information over unsecured computer messaging systems, networks and other pathways creates a vulnerability that is actively being exploited by the enemy in all theatres. While sending orders via AOL may seem extreme, there have been similar instances – and even worse – security violations. Anyone using a computer or other communication system has to think past the orders, regulations and whatever your commander tells you in the morning briefing. This is simply a matter of common sense. What you upload, key in, or transmit in any other way is being actively and constantly monitored. All personnel need to use extreme caution when deciding what information and materials to send via unsecured means.

Maintaining OPSEC is not a responsibility assigned to any individual, rank or task. It is critical that all personnel do their part in keeping information from the enemy whether they are in theater or sitting in a stateside base. AR 25-2 is a critical force protection resource that is as important as any weapons system or tactical guide.

On Cyber Patrol is a recurring graphic training aid that highlights key concepts and components of information assurance as covered by AR 25-2. For more information or to receive your own copy for training and motivational activities please contact oncyberpatrol@hqda.army.mil or visit the Army Information Assurance web site on Army Knowledge Online (AKO) at HYPERLINK https://informationassurance.us.army.mil/.